UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,485	02/09/2004	Ramarathnam Venkatesan	MS1-1922US	2829

22801 7590 02/07/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	02/07/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 02/07/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/775,485	VENKATESAN ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 4/9/04 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/09/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response of the original filing of February 9, 2004. Claims 1-38 are pending and have been considered below.

Double Patenting

1. Claim 7 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 3. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Objections

2. Claims 21, 26 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Claims 21 and 26 are product claims (i.e. computer-readable media) that refer back to Claims 15 and 22. The Office considers any claim that refers to another claim as dependent thereon, i.e. a dependent claim. Since Claims 15 and 22 are method claims comprising a couple of steps and Claims 21 and 26 fail to add, delete, or change any of these steps, Claims 21 and 26 fail to further limit the parent claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 22 recites the limitation "the node matrix" in claim 22. There is insufficient antecedent basis for this limitation in the claim.

Examiner note

The applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in claims 27, 29 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer programs modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Specification

4. 35 U.S.C. 112, first paragraph, requires the specification to be written in "full, clear, concise, and exact terms." The specification is replete with terms which are not clear, concise and exact. The specification should be revised carefully in order to comply with 35 U.S.C. 112, first paragraph. Examples of some unclear, inexact or

verbose terms used in the specification are: in paragraph 23, the used of **if** instead of and so on. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-5, 7, 8, 31-35, 37, 38 are rejected under 35 U.S.C. 102(b) as being anticipated by **Menezes et al** from Handbook of applied cryptography ISBN 0-8493-8523-7.

Claims 1, 31: **Menezes et al** discloses a secure hash function comprising:

Applying a block function to a first data input block from a plurality of data input blocks (fig 9.2 a and b) (page 332);

And applying the block function to a second data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block (fig 9.2 a and b) (page 332).

Claims 2, 32: **Menezes et al** discloses a secure hash function as in claims 1 and 31 above, and further discloses that the method provide a secure hash function

(Hash function are used for data integrity in conjunction with digital signature schemes) (page 321, paragraph 3).

Claims 3, 33: **Menezes et al** discloses a secure hash function as in claims 1 and 31 above, and further discloses that the plurality of data input blocks is formed by dividing an input string (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332).

Claims 4, 34: **Menezes et al** discloses a secure hash function as in claims 1 and 31 above, and further discloses that each of the plurality of data input blocks has a fixed length (each block xi then serves as input to an internal fixed size hash function) (page 332 and fig 9.2b).

Claims 5, 35: **Menezes et al** discloses a secure hash function as in claims 1and 31 above, and further discloses that one or more of the plurality of data input blocks are padded as needed to provide a fixed length for each of the data input blocks (this preprocessing typically involves appending extra bits (padding) as necessary to attain an overall bit length (pages 332).

Claims 7, 37: **Menezes et al** discloses a secure hash function as in claim 1 above, and further discloses that the plurality of data input blocks is formed by

dividing an input string (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332).

Claims 8, 38: **Menezes et al** discloses a secure hash function as in claims 1, 31 above, and further discloses:

a. Dividing an input string to provide the plurality of data input blocks (each block xi then serves as input to an internal fixed size hash function) (page 332 and figure 9.2b);

b. And determining a hash value of the input string, the hash value corresponding to a result provided by the application of the block function to a last data input block (figure 9.2 a and b).

7. Claims 9, 11, 12, 22, 26 are rejected under 35 U.S.C. 102(b) as being anticipated by **Rosen** Discrete mathematics and its applications second edition ISBN 0-07-053744-5 in 1991.

Claim 9: **Rosen** teaches a method on multiplying matrix and generating graph comprising:

Providing a graph corresponding to a data input block (the concept of interior vertices of path is used in the warshall's algorithm to generate a graph (page 373);

Labeling each outgoing edge of every node in the graph with a label (page 368, figure 1);

And tracing a path through a plurality of labels on the graph, the path being defined by a sequence of elements within the input block (page 368, figure 1).

Claim 11: **Rosen** teaches a method on multiplying matrix and generating graph and further teaches that the graph has a degree d (page 370, figure 2).

Claim 12: **Rosen** teaches a method on multiplying matrix and generating graph and further teaches that the labels are integer labels (for some positive integer i with i <= n) (page 371, paragraph 3).

Claims 22, 26: **Rosen** teaches a method on multiplying matrix and generating graph comprising:

a. Labeling each node of a graph with a matrix (page 375, figure 4);

b. Navigating to a next node of the graph (page 375, figure 4);

c. And multiplying the node matrix by at least one of a plurality of generator matrices (Warshall's algorithm) (pages 373-375).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Rosen** Discrete mathematics and its applications second edition ISBN 0-07-053744-5 in 1991.

Claim 13: **Rosen** teaches a method on multiplying matrix and generating graph and further teaches page 370, figure 2), but does not explicitly teaches that each of the integer labels has a value less than or equal to d. Additionally, the examiner considers it is immaterial as to compare the integer value and the degree of the graph. It would have been obvious to one having ordinary skills in the art at the time the invention was made to make the angle smaller than the value of the labels. One would have been motivated to do so in order to maintain data integrity since small angle are used in trigonometry in control function in order to reduce the error rate.

10. Claims 10, 14-19-21, 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Rosen** Discrete mathematics and its applications second edition ISBN 0-07-053744-5 in 1991 in view of **Menezes et al** from Handbook of applied cryptography ISBN 0-8493-8523-7.

Claim 10: **Rosen** teaches a method on multiplying matrix and generating graph as in claim 9 above, but does not explicitly teach that the tracing ends at a point that indicates a value of a compression function for a secure hash implementation. However, **Menezes et al** discloses a secure hash function that further discloses that the tracing ends at a point that indicates a value of a compression function for a secure hash implementation (hash function h is designed as iterative processes which hash arbitrary length inputs by processing successive fixed sized blocks of the input as illustrated in figure 9-2) (page 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to indicate the hash value to be the last value of the iteration. One would have been motivated to do so in order to maintain data integrity.

Claim 14: **Rosen** teaches a method on multiplying matrix and generating graph as in claim 9 above, but does not explicitly teach that the input block is a portion of an input string. However, **Menezes et al** discloses a secure hash function that further discloses that the input block is a portion of the input string (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to divide the input string in

input blocks. One would have been motivated to do so in order to maintain data integrity.

Claims 15, 21: **Rosen** teaches a method on multiplying matrix and generating graph comprising:

a. Constructing a table of entries (page 430, table 1, and 2);

b. Setting an initial matrix to an identity matrix (Warshall's algorithm is based on the construction of sequence of zero-one matrices. These matrices are Wo, W1, ... Wn, where W0 =Mr is the zero-one matrix of this relation) (page 373);

c. Indexing each block to a generator matrix represented in the table(page 430, table 1 and 2);

d. And updating the initial matrix (page 376, Algorithm 2).

But does not explicitly teaches a step of processing input data as one or more blocks of fixed length (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). However, **Menezes et al** discloses a secure hash function that further discloses a step of processing input data as one or more blocks of fixed length (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to process input of

fixed size. One would have been motivated to do so in order to make the process efficient.

Claim 16: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claim 15 above, and **Menezes et al** further discloses that the method is utilized to provide a secure hash function (Hash function are used for data integrity in conjunction with digital signature schemes) (page 321, paragraph 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to include a secure hash function. One would have been motivated to do so in order to maintain data integrity.

Claim 17: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claim 15 above, and **Menezes et al** further discloses that the data encryption standard (DES) is utilized to provide an inter-block function for the blocks. Additionally, the Examiner considers it immaterial as to which encryption standard is used and that it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Menezes et al** to use DES. One would have been motivated to do so in order to maintain data integrity.

Claim 18: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claim 15 above, and **Rosen** further teaches that the updating is performed by multiplying the initial matrix by the index matrix (a matrix multiplication algorithm) (page 147, 148). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Menezes et al** to use matrix multiplication for updating purpose. One would have been motivated to do so in order to maintain system efficiency.

Claim 19: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a secure hash function as in claim 15 above, and **Rosen** further teaches that the table comprises entries for all possible products plurality of generator matrices (the used of incidence (generator) matrices to represent graphs) (page 432 and 433). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Menezes et al** to use matrix multiplication for updating purpose. One would have been motivated to do so in order to maintain system efficiency.

Claim 23: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claim 22 above, and **Menezes et al** further discloses that the method is used to provide a stream cipher implementation (a linear complexity steam cipher is discuss on

pages 198-200). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to provide a stream cipher. One would have been motivated to do so in order to maintain data integrity.

Claim 24: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claim 22 above, and **Menezes et al** further discloses that the method is used to determining a hash value corresponding to a sequence of intermediate nodes of the graph (a linear complexity steam cipher is discuss on pages 198-200). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to provide a stream cipher. One would have been motivated to do so in order to maintain data integrity.

Claims 20, 25: **Rosen** and **Menezes et al** disclose a method on multiplying matrix and generating graph and a method for producing a secure hash function as in claims 15 and 22 above, and **Rosen** further discloses that the plurality of generator matrices is free monoid (Warshall's algorithm is based on based on the construction of a sequence of zero-one matrices with similar property) (page 373, paragraph 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** and **Menezes et al** to

provide generator matrices with a free monoid properties. One would have been motivated to do so in order to maintain data integrity.

1. Claims 6, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Menezes et al** from Handbook of applied cryptography ISBN 0-8493-8523-7.

in view of **Rosen** Discrete mathematics and its applications second edition ISBN 0-07-053744-5 in 1991

Claims 6,36: **Menezes et al** discloses a secure hash function as in claims 1 and 31 above, but does not discloses that the block function is based on a walk on a graph defined by a plurality of matrices. However, **Rosen** discloses a method on multiplying matrix and generating graph and further discloses that the warshall's algorithm can be used to trace a path (pages 373-375). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Menezes et al** to provide block function based on a walk on a graph. One would have been motivated to do so in order to maintain system efficiency.

11. Claims 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Aiello et al** (US 5892829) in view of **Menezes et al** Hash function and data integrity chapter 9 from Handbook of applied cryptography 1996.

Claim 27: **Aiello et al** discloses a secure hash function comprising:

A processor (figure 1);

A system memory coupled to the processor (figure 1);

But does not explicit disclose a means for applying a block function to a first and second data input block from a plurality of data input blocks. However, **Menezes et al** discloses a similar system that further discloses a means for applying a block function to a first data input block from a plurality of data input blocks (fig 9.2 a and b) (page 332).

And a means for applying the block function to a second data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block (fig 9.2 a and b) (page 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Aiello et al** to include a means for applying a block function to a first and second data input block from a plurality of data input blocks. One would have been motivated to do so in order to maintain data integrity.

Claim 28: **Aiello et** al and **Menezes et al** disclose a secure hash function as in claim 27 above, and **Aiello et al** further discloses that the system is utilized to provide at least one item selected from a group comprising a secure hash function and a stream cipher (a compression function to provide a secure hash function) (abstract). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made for **Aiello et al** to include a means for applying a block function to a first and second data input block from a plurality of data input blocks. One would have been motivated to do so in order to maintain data integrity.

Claim 29: **Aiello et** al and **Menezes et al** disclose a secure hash function as in claim 27 above, and **Menezes et al** further discloses a means for dividing an input string to provide the plurality of data input blocks (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Aiello et al** to include a means dividing the input string to a plurality of data input blocks. One would have been motivated to do so in order to maintain data integrity.

Claim 30: **Aiello et** al and **Menezes et al** disclose a secure hash function as in claim 27 above, and **Menezes et al** further discloses a means for dividing an input string to provide the plurality of data input blocks (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332), and means for determining a hash value of the input string, the hash value corresponding to a result provided by the application of the block function to a last data input block(figure 9.2 a and b). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Aiello et al** to

include a means dividing the input string to a plurality of data input blocks. One would have been motivated to do so in order to maintain data integrity.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

c. Feistel (US 4316055) discloses a stream/block cipher cryptographic system.

d. Moreau (US 6069954) discloses a cryptographic data integrity with serial bit processing and pseudorandom generators.

e. Coppersmith et al (US 2003/0152219) disclose an efficient stream cipher and method.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
February 1, 2007

James W. Myhre
Supervisory Patent Examiner